

1
2
3 FILED ENTERED
4 LODGED RECEIVED
5

MAR 11 2013

6 AT SEATTLE
CLERK U.S. DISTRICT COURT
7 BY WESTERN DISTRICT OF WASHINGTON
DEPUTY

8 UNITED STATES DISTRICT COURT
9 WESTERN DISTRICT OF WASHINGTON
10 AT SEATTLE

11 UNITED STATES OF AMERICA,) CASE NO. *MJ13-138*
12)
13 Plaintiff,) COMPLAINT for VIOLATION
14)
15 v.)
16) Title 18, United States Code,
17) Sections 1029(a)(3) and 2
18)
19)
20 Defendants.)

21 BEFORE the Honorable James P. Donohue, United States Magistrate Judge, U.S. Courthouse,
22 Seattle, Washington.

23 The undersigned complainant being duly sworn states:

24 **COUNT 1**
25 **(Possession of Counterfeit or Unauthorized Access Devices)**

26 *2013 Mar JPD*

27 On February 5, ~~2012~~, at Seattle, within the Western District of Washington, the
28 defendants, CHRISTOPHER ROLON-GONZALES and SANTIAGO ZAYCO, knowingly, and
with intent to defraud, possessed fifteen or more counterfeit and unauthorized access devices, to
wit: counterfeit credit/debit cards, account numbers, personal identification numbers, and other
means of account access that can be used, alone and in conjunction with another access device, to
obtain money, goods, services, and any other thing of value, and that can be used to initiate a

1 transfer of funds; said activity affecting interstate and foreign commerce.

2 All in violation of Title 18, United States Code, Sections 1029(a)(3) and 2.

3

4 And the complainant states that this Complaint is based on the following information:

5 I, John Wurster, being first duly sworn on oath, depose and say:

6

7 **I. BACKGROUND**

8 1. I am a Special Agent with the United States Secret Service (USSS) and have been
9 so since June 21, 1999. I am currently assigned to the Seattle Field Office. I am a graduate of
10 the Federal Law Enforcement Training Center located in Glynco, Georgia, and the United States
11 Secret Service, Special Agent Training Program located in Beltsville, Maryland. Prior to my
12 employment with the Secret Service, I served in the United States Army as a Counterintelligence
13 Special Agent. I have a Bachelor of Science Degree from Brenau University. As part of my
14 training with the Secret Service, I have received instruction on the investigation of financial
15 crimes, including credit/debit card fraud, mail and wire fraud, access device fraud and identity
16 theft. I have also completed specialized training in the investigation of electronic crimes
17 involving the use of computers and other electronic devices. In the course of my law
18 enforcement career, I have investigated crimes ranging from the production and passing of
19 counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the
20 President and Vice President of the United States. As part of my duties, I also investigate
21 criminal violations relating to child exploitation and child pornography, including violations
22 pertaining to the illegal production, distribution, receipt, and possession of child pornography and
23 material involving the sexual exploitation of minors in violation. I am a member of the Seattle
24 Internet Crimes Against Children Task Force, and work with other federal, state, and local law
25
26
27
28

enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. This Affidavit is made in support of a complaint for the arrest of CHRISTOPHER ROLON-GONZALES and SANTIAGO ZAYCO, for violations of Title 18, United States Code, Section 1029(a) (Access Device Fraud). The information contained in this Affidavit is based on my own personal knowledge and information provided to me during my participation in this investigation, including information provided by other law enforcement officers and witnesses. This Affidavit is submitted solely for the purpose of establishing probable cause for the charge alleged in this Complaint and does not purport to set forth all of my knowledge of, or investigation into, this case.

II. INVESTIGATION

3. This case involves a skimming operation in which card data is stolen in Canada and encoded onto white plastic cards. These same cards are then transported into the United States, where they are provided to other suspects who withdraw funds from ATMs in a "cash out" scheme. Early estimates from the victim banks showed \$209,210.57 in actual loss was attributed to this group, with over \$385,659.31 in attempted loss. I expect that the continuing investigation will uncover additional attempted and actual loss.

A. Background: Skimming and Skimming Devices

4. Generally speaking, credit/debit card "skimming" is the theft of credit/debit card information used in an otherwise legitimate transaction. Among other techniques, suspects often use a small device (the "skimmer" or "skimming device") to steal data the information, or track data, of an unsuspecting victim's credit/debit card. Skimming devices are often capable of holding data pertaining to hundreds or even thousands of bank cards.

1 5. After stealing card data, suspects will connect the skimming devices to a
2 computer, and then download the victim account data. Typically, suspects will then transfer or
3 "re-code" victim card data onto blank credit/debit card stock, also known as "white plastic."
4
5 Suspects have also been known to re-code stolen card data onto store gift cards or other
6 credit/debit cards. Virtually any plastic card with a magnetic stripe on the back of the card may
7 be used to re-code victim card data and access funds and/or credit on the victim's account. Given
8 the nature of the activity, skimming necessarily requires use of a computer and other digital
9 devices, including encoding equipment and software and USB devices.
10

11 6. Once this process is complete, suspects use the newly made counterfeit cards,
12 sometimes called "white plastic cards," to access victim's accounts at ATM machines or through
13 point-of-sale purchases. Typically, suspects will use victim information to withdraw cash and/or
14 make purchases within a short period of time from the date that the credit/debit card account was
15 "skimmed." In some instances, however, suspects will wait several months before utilizing the
16 stolen data. In either case, however, suspects will typically conduct numerous fraudulent
17 transactions in a short time frame in order to maximize the use of the stolen data before the
18 financial institution or the individual victim account holder recognizes the breach and begins
19 shutting down the compromised accounts.
20

21 **B. Evidence of Criminal Activity**

22 7. This investigation originated on December 9, 2012, when a Boeing Employees
23 Credit Union (BECU) Investigator identified a group of individuals performing cash out fraud at
24 BECU ATMs in and around Seattle. BECU gathered surveillance photos and a list of card
25 numbers being used at BECU ATMs. An examination of the card numbers revealed that they all
26 related to debit cards and accounts at VanCity Credit Union of Vancouver, British Columbia.
27
28

1 8. The United States Secret Service (USSS) Vancouver Resident Office contacted
 2 VanCity investigators concerning the debit cards used in and around Seattle at the BECU ATMs
 3 and it was determined that these cards had been compromised from various coffee shops in
 4 Vancouver, to include The Dirty Apron Coffee and multiple Starbucks locations.
 5

6 9. Following this initial video dump from BECU, it appeared that the same
 7 individuals were performing cash outs in Seattle with Canadian debit cards on a regular basis.
 8 The cash out dates typically were on weekends, such as the weekends of December 1, 2012;
 9 December 9, 2012; January 5, 2013; January 20, 2013; and February 2, 2013. According to the
 10 Royal Canadian Mounted Police (RCMP), it has verified at least 11 common points of purchase
 11 (and compromise) involved in this investigation, as well as additional suspected points of
 12 compromise.
 13

14 10. On January 5, 2013, the RCMP contacted the USSS Vancouver Resident Office
 15 requesting assistance with the investigation of T.G., a Canadian citizen. The Canadian Border
 16 Services Agency had intercepted T.G. with 22 "white plastic cards" containing TD Bank data and
 17 \$12,000.00 at the Douglas Border Crossing. Inside T.G.'s phone was the name "Dennis."
 18 According to their intelligence files, "Dennis" was "Dennis Nguyen." They also reported finding
 19 several phone numbers for area codes in Washington State.
 20

21 11. According to border crossing records, Dennis Nguyen made at least eight border
 22 crossings from Canada into the United States since November 2012. In each instance he was
 23 driving the same 2008 Jeep Cherokee with a British Columbia license plate.
 24

25 12. On February 5, 2013, the USSS Seattle Field Office was notified that the Royal
 26 Bank of Canada (RBC) reported a mass cash out attempt in progress at numerous ATMs in the
 27 downtown Seattle area. RBC provided real time data of where the transactions were taking
 28

1 place, which enabled JP Morgan Chase Bank central fraud monitoring to provide a photograph
 2 and description of a suspect. Surveillance videos showed the suspect, a Hispanic male with dark,
 3 spiked hair, wearing a black jacket and jeans, conducting the cash-outs at various ATMs.
 4

5 13. A search of the areas near these ATMs was initiated. Detective David Dunn of
 6 the Seattle Police Department and USSS Special Agent Bryan Molnar located the suspect at an
 7 ATM on 4th Ave in Westlake Park in downtown Seattle. The suspect, identified as Santiago
 8 Zayco, was contacted and taken into custody. A search incident to arrest yielded 49 "white
 9 plastic cards" and \$1,620.00 in cash wrapped around ATM receipts found on Zayco's person. It
 10 should be noted the "white plastic cards" had no bank markings or printing on the front or back,
 11 just a magnetic strip. A white label was printed on the front of each card with what appeared to
 12 be the PIN on it. I know from my training, experience and other investigations that "white plastic
 13 cards" are used by skimmers and other types of fraud suspects to encode information and then
 14 withdraw money or purchase items.
 15

16 14. Santiago Zayco was transported to the USSS Seattle Field Office, where he agreed
 17 to be interviewed. Agent Molnar read Zayco his Miranda Rights, which Zayco stated he
 18 understood. Zayco agreed to speak with law enforcement. Agent Molnar asked Zayco how he
 19 had traveled downtown and asked if he was alone. Zayco stated he was alone at the time we
 20 contacted him, but his cousin's husband was coming to the area to do cash outs with him. Agent
 21 Molnar asked Zayco for consent to search his car and read him a "consent to search" form.
 22 Zayco agreed and signed the consent form. Zayco informed Agent Molnar his car was parked
 23 underneath the Pacific Place Mall in the parking garage, on the lowest level.
 24

25 15. USSS Special Agent Malcolm Frederick and I located Zayco's vehicle, where
 26 Zayco had described, and initiated the search. Inside Zayco's vehicle, Agent Frederick and I
 27

1 found 169 white plastic credit cards and \$6,340.00 in cash wrapped around ATM receipts. While
 2 we were searching the car, Agent Frederick observed a male driving a black Mercedes watching
 3 us as he slowly drove through the parking garage.
 4

5 16. Upon completion of the search, I advised Agent Molnar of the results. During
 6 subsequent questioning, Agent Molnar asked Zayco about the items found in the car. Zayco
 7 admitted the money found in the car was obtained from the illegal cash out scheme and the white
 8 plastic cards were provided to him by "Dennis" to do the cash outs. Zayco admitted he used
 9 some of the money he obtained from the cash-outs to purchase his vehicle, along with funds left
 10 to him by his father. Zayco admitted his actions were stupid but stated he was a poor student and
 11 needed money.
 12

13 17. Santiago Zayco stated the cards found on his person were given to him by
 14 "Dennis." Zayco said he would meet with "Dennis" every week or two. Zayco said "Dennis"
 15 would give him new cards and Zayco would give "Dennis" the cash he obtained from doing
 16 cash-outs with the prior week's cards, along with the corresponding ATM receipts. Zayco said he
 17 would be given a portion of the cash from the cash outs as payment. Zayco said he corresponded
 18 with "Dennis" by a "burner" cellular telephone that "Dennis" would provide him. Zayco said that
 19 phone was in his pocket when we contacted him. Zayco also stated "Dennis" would give him
 20 new phones periodically and take the old phones back. Agent Molnar asked Zayco for consent to
 21 forensically search the phone. Zayco gave consent and signed a "consent to search" form. The
 22 phone was imaged by Detective Chris Hansen of Seattle Police Department as the interview
 23 progressed. I know from my training and experience that individuals involved in criminal
 24 activities may utilize pre-paid cellular phones due to the anonymity such devices may provide.
 25 These phones do not require a contract with a telephone service provider that could be researched
 26
 27
 28

1 for account billing information. Instead, following the initial cash purchase of such a phone at
 2 any number of retail stores, these phones may be loaded with minutes and/or days of service via
 3 the cash purchase of gift cards associated with the provider of the cell phone. The terms "burner
 4 and "burn phone" are related to the ease with which suspects can discard such phones if they
 5 believe they may be arrested or "burned."

7 18. Zayco was shown surveillance videos of himself from prior cash outs. Zayco
 8 admitted to performing the cash-outs. He was shown surveillance photos of other people in this
 9 group who had been using cards encoded with stolen account information to make cash outs.
 10 Zayco identified his cousin's husband, Chris Rolon-Gonzales (Rolon), from a surveillance video
 11 of Rolon performing a cash out with a stolen account white plastic card. Zayco stated he and
 12 Rolon met a "cousin's cousin" named T.G. (same as above) at a family wedding. T.G. told them
 13 he could help them get some money and set up a meeting with a man named "Dennis." Zayco
 14 was shown a surveillance photograph of Dennis Nguyen, provided by the USSS Vancouver
 15 Resident Office, and Zayco identified Nguyen as the person known to him as "Dennis."
 16

18 19. While being interviewed, Zayco received multiple phone calls from Chris Rolon,
 20 who was supposed to be meeting him to do cash outs. Rolon advised he left the area and was
 21 scared because he saw people searching Zayco's vehicle. Zayco arranged a meeting with Rolon
 22 in downtown Seattle. Zayco provided law enforcement with a description of Rolon and his
 23 vehicle, a black Mercedes. Agent Frederick advised this was the male who had been watching
 24 while he and I searched Zayco's car.

25 26. Upon his arrival to the prearranged meeting location, Chris Rolon was taken into
 27 custody. He was transported to the USSS Seattle Field Office, where he agreed to be
 28 interviewed. Agent Molnar read Rolon his Miranda Rights. Rolon stated he understood his

1 rights and would speak with law enforcement.

2 21. Agent Molnar asked Rolon for consent to search his vehicle. Rolon gave written
 3 consent to a search of his vehicle. Agent Molnar asked Rolon if there was any contraband in the
 4 vehicle. Rolon stated we would find cash in the car. I asked him where he obtained the money,
 5 and Rolon admitted it was from doing cash outs. While conducting the search of Rolon's
 6 vehicle, USSS Special Agent David Mills and Agent Frederick located \$4,760.00 in cash and
 7 ATM receipts hidden in a gym bag in the trunk of the car.
 8

9 22. During the interview, Rolon admitted to doing the cash outs and claimed he met a
 10 "cousin's cousin" at a family wedding named T.G. Rolon stated T.G. said he could help Rolon
 11 earn some money. T.G. set up a meeting with a man named "Dennis." Rolon was shown a
 12 surveillance photograph of Dennis Nguyen, provided by the USSS Vancouver Resident Office,
 13 and Rolon identified Nguyen as the person known to him as "Dennis."
 14

15 23. Rolon stated he and Zayco typically would meet with Nguyen every week or two.
 16 Rolon said he and Zayco would share a cell phone in which they would communicate with
 17 Nguyen through text messages and calls. Rolon said they typically met was at hotel rooms on the
 18 west side of Interstate 5 near Northgate Mall, where Nguyen gave them counterfeit cards. Rolon
 19 was shown photographs of other people doing cash-outs. Rolon identified Zayco as well as
 20 others.
 21

22 24. Rolon and Zayco later told agents that Nguyen left a red bag with them, which
 23 they provided to Nguyen when he traveled to Washington. Rolon and Zayco provided the bag to
 24 USSS. A search of that bag yielded \$77,140.00 in cash, 332 white plastic credit cards (most of
 25 which had a printed label with the cards' associated PIN numbers printed on it), seven cell phones
 26 of the same make and model, a cash counting machine, a credit card magnetic strip encoder, a
 27
 28

1 label printer, label printing software, 12 rolls of white label tape, and miscellaneous supplies.
2 Based upon my training, experience and my examination of the evidence contained in the red
3 bag, I know the credit card magnetic strip encoder, "white plastic cards", label printer and blank
4 labels are used in the production of counterfeit access devices.
5

6 25. On February 11, 2013, Dennis Nguyen crossed the border into the United States
7 and traveled to the Seattle area where he had arranged to meet Zayco and Rolon. Nguyen was
8 arrested near Northgate Mall. In his possession was a laptop computer.
9

10 26. A forensic analysis of that computer thus far has uncovered over 2,600
11 credit/debit card numbers on the hard drive. Moreover, USSS has recovered 678 "white plastic
12 cards" and about \$89,860 in cash directly related to this investigation. Of those "white plastic
13 cards," 677 were encoded with account data and are thus counterfeit cards (or "counterfeit access
14 devices," as defined by federal law), while one card was blank. The investigation remains
15 ongoing.
16

17 //

18 //

19 //

20

21

22

23

24

25

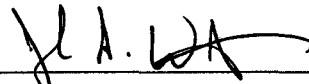
26

27

28

1 **III. CONCLUSION**

2 27. Based on the above facts, I respectfully submit that there is probable cause to
3 believe that CHRISTOPHER ROLON-GONZALES and SANTIAGO ZAYCO did knowingly
4 and intentionally committed the offense of access device fraud, in violation of Title 18, United
5 States Code, Sections 1029(a) and 2.

6 
7 JOHN WURSTER, Complainant
8 Special Agent, United States Secret Service

9
10
11 Based on the Complaint and Affidavit sworn to before me, and subscribed in my
12 presence, the Court hereby finds that there is probable cause to believe the Defendant committed
13 the offense set forth in the Complaint.

14 Dated this 11th day of March, 2013.

15
16 
17 HON. JAMES P. DONOHUE
18 United States Magistrate Judge
19
20
21
22
23
24
25
26
27
28